10

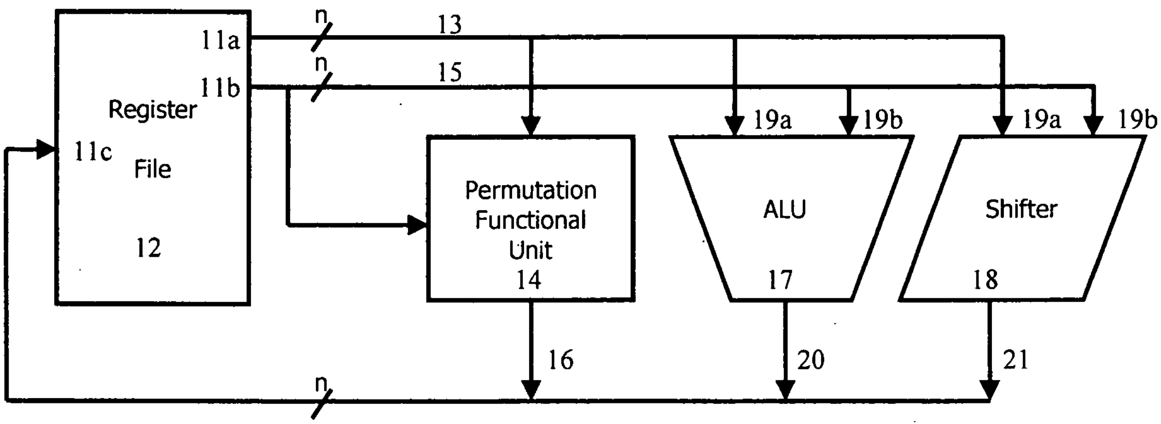
Register
File
12
11a
11b
11c
n
13
15
Permutation
Functional
Unit
14
ALU
17
Shifter
18
19a
19b
16
20
21

FIG. 1

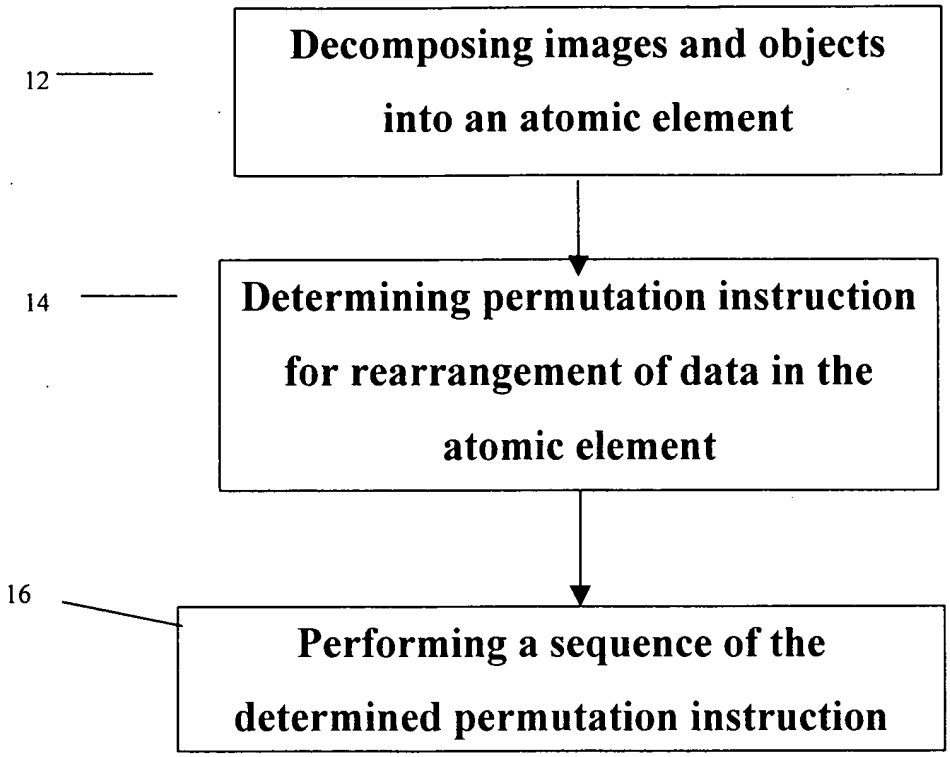

FIG. 2

(a) Area mapping of a 4x4 matrix:

R1 =	a00	a01	a02	a03
R2 =	a10	a11	a12	a13
R3 =	a20	a21	a22	a23
R4 =	a30	a31	a32	a33

Fig. 3a

(b) Decomposition into four 2x2 matrices:

R1 =	a00	a01	b00	b01
R2 =	a10	a11	b10	b11
R3 =	c00	c01	d00	d01
R4 =	c10	c11	d10	d11

Fig. 3B

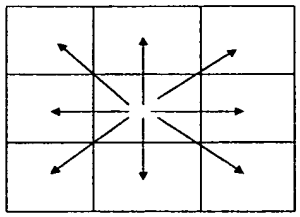

Fig. 4A

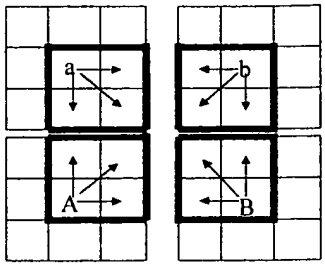

Fig. 4B

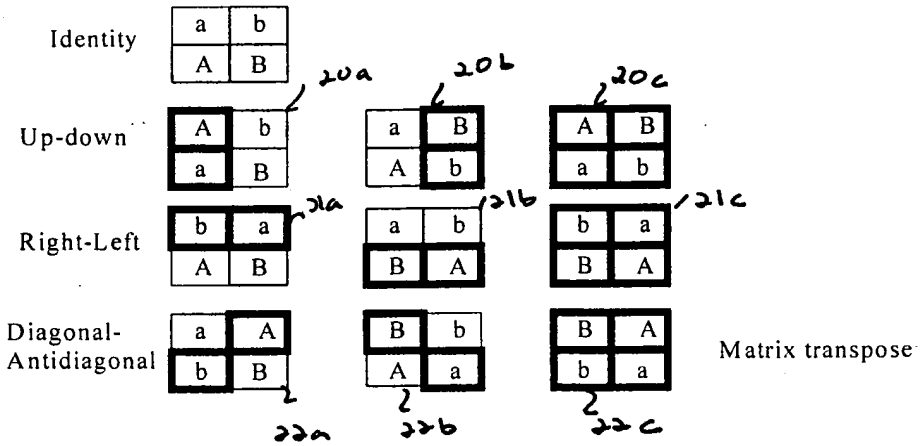

Fig. 4C

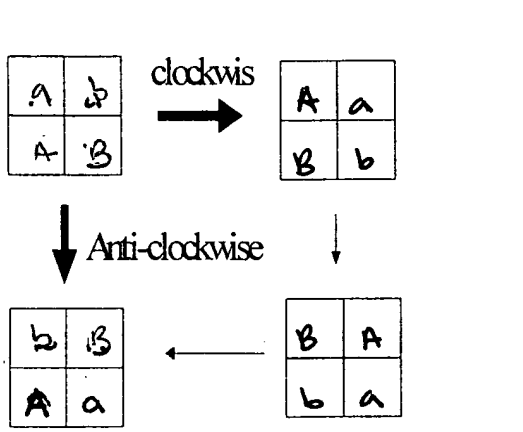

Fig. 5A

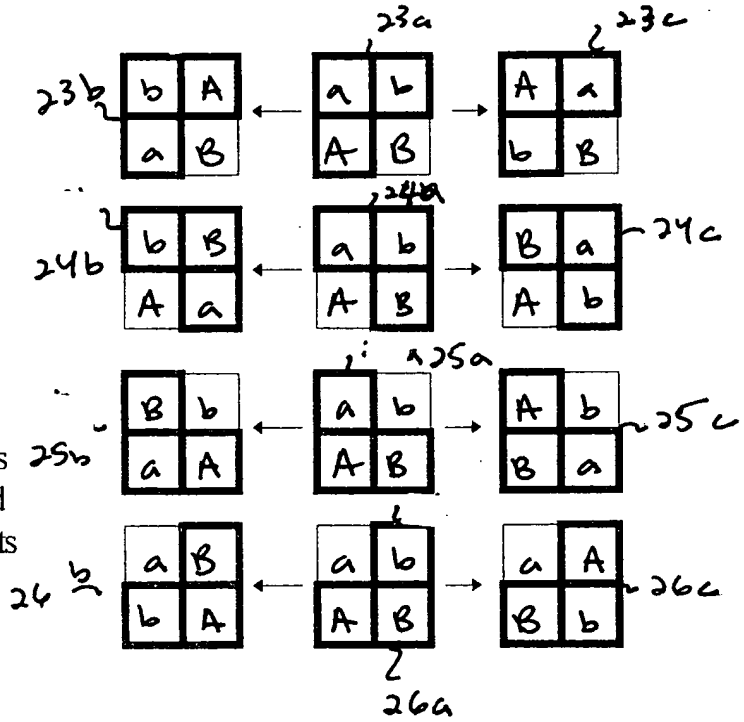

Fig. 5B

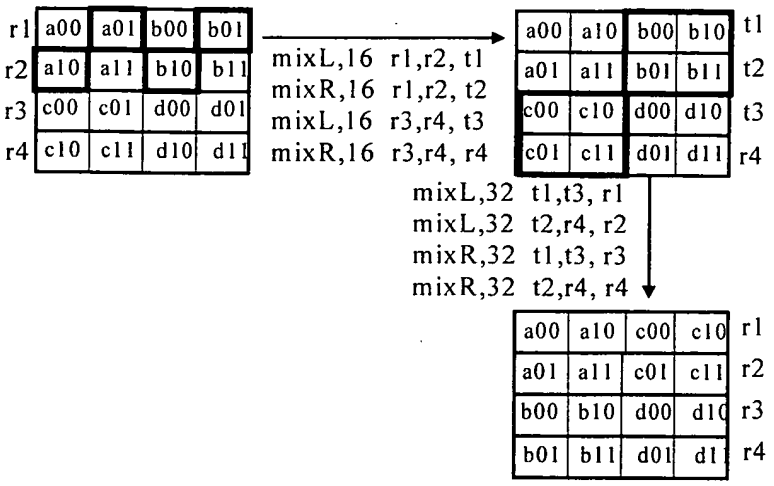

Fig. 6:

Identity

a	b
A	B

Changing Rows to Diagonals

b	A
B	a

B	a
b	A

Changing Diagonals to Columns

B	A
a	b

A	B
b	a

Figure7

Alphabet A:

mixL, **mixR** on 8, 16 and 32 bit subwords (or **cmixL**, **cmixR**)
check on 8, 16 and 32-bit subwords (or **ccheck**)
excheck on 8, 16 and 32-bit subwords (or **cexcheck**)
permset on 8, 16 and 32 bit subwords, with 4-element sets (or **cexchange**)

Fig. 8A

Alphabet B (minimal):

mixL, **mixR** on 8, 16 and 32 bit subwords (or **cmixL**, **cmixR**)
permset on 8, 16 and 32 bit subwords, with 4-element sets (or **cexchange**)

Fig. 8B